INTERVIEW

Jörg Vollmer,
Account-Manager,
Qualys

Systemschwächen dokumentieren

Gegenmaßnahmen – Die Zahl der Patches hat Ausmaße angenommen, die kaum noch handhabbar sind. Jörg Vollmer, Account-Manager beim Audit-Dienstleister Qualys, erklärt, warum es immens wichtig ist, diese Aufgabe zu lösen.

Security-Forum: Warum ist ein Vulnerability-Management wichtig?

Vollmer: Ungepatchte Systeme haben messbare Einflüsse. Ein gutes Beispiel ist der neulich ausgebrochene Wurm »Zotob«. Er hat vor allem in der Amerikanischen Industrie größere Geschäftsausfälle verursacht. Insbesondere ungepatchte Systeme haben die Verbreitung dieses Wurmes erst ermöglicht. Ein Vulnerability-Management-Konzept (VM) deckt die verwundbaren Plattformen strukturiert auf.

Security-Forum: Worauf sollten IT-Verantwortliche beim Einsatz einer VM-Lösung achten?

Vollmer: Da ein VM-System nicht nur Schwachstellen aufspürt, sondern als integraler Bestandteil eines Sicherheitsprozesses innerhalb des Unternehmens eingesetzt wird, muss es mehrere Kriterien erfüllen.

Auf Grund der schnellen Entwicklung von Exploits für Schwachstellen sollten Signaturen für kritische Varianten innerhalb von 24 Stunden verfügbar sein. Dabei ist eine niedrige False-Positive-Rate obligatorisch. Die Multi-User-Fähigkeit und zentrales Management sind für einen globalen VM-Prozess ein Muss, damit alle Updates und Informationen ohne Verzögerung verfügbar sind. Schwachstellenreports und Trendanalysen sollten von den verantwortlichen Personen immer und überall abrufbar sein. Um mit dem Wachstum des Unternehmens und des Netzwerks mithalten zu können, muss das System ohne großen Aufwand erweiterbar sein. Das Steuerungs-Interface muss einfach bedienbar und die Reports rasch zu erfassen sein, um schnellstmöglich zu guten Ergebnissen zu kommen.

Security-Forum: Welche sind die Leitfäden bei Einsatz einer VM-Lösung?

Vollmer: VM bedeutet Identifizieren, Priorisieren und Beheben von Schwachstellen. Viele Unternehmen haben in der Zwischenzeit einen Prozess für das Schwachstellenmanagement im Einsatz, welcher sechs Schritte umfasst:

1. Erkennung der aktiven Geräte im Netzwerk, um die Topologie und eventuelle Veränderungen verfolgen zu können
2. Priorisierung von Assets, um die Relevanz der einzelnen Systeme und Gruppen zu definieren
3. Analyse und Auswertung: umfassende Analyse der Systeme nach vorhanden Schwachstellen und Beurteilung, wie kritisch diese für das System und Netzwerk sind
4. Beheben der Schwachstellen, beispielsweise durch Einspielen von Patches oder das Durchführen von Workarounds
5. Verifizierung: durch erneutes Überprüfen feststellen, ob die Patches oder Workarounds das gewünschte Ergebnis bringen
6. Policy-Compliance: Beurteilung des Sicherheitsstandards durch Gegenüberstellung der Ergebnisse mit Security-Policy-Vorgaben und Compliance-Anforderungen wie Sox oder Hipaa ◆